Bessere Ausfallsicherheit bei Cyberangriffen und Schutz Ihrer Daten vor Ransomware-Cyberbedrohungen durch Nutzung eines isolierten Vault, einer KI-basierten ML-Analysesoftware und mehr

Mit Dell Technologies PowerProtect Cyber Recovery mit CyberSense

Da die Häufigkeit von Cyberbedrohungen kontinuierlich zunimmt und sich Angriffsmethoden weiterentwickeln, müssen Data-Protection-Pläne einen Ansatz verfolgen, mit dem alle IT-Komponenten gesichert und analysiert werden – von den oberflächlichsten bis hin zu den tiefsten Bereichen. Dell PowerProtect Cyber Recovery kann dazu beitragen, die kritischsten und sensibelsten Daten zu schützen und gleichzeitig eine ordnungsgemäße Recovery bei einem Cyberangriff oder einem anderen unterbrechenden Ereignis sicherzustellen.

Dell PowerProtect Cyber Recovery ist eine Datenmanagement-, Schutz- und Recovery-Lösung, mit der Unternehmen ihre Daten und Anwendungen vor Ransomware, destruktiven Cyberangriffen und unerwarteten Ereignissen schützen können. Die Lösung basiert auf einem Multi-Copy-Ansatz, was bedeutet, dass Backups nach der Erstellung zur Sicherung und Analyse in einen isolierten Storage kopiert werden. PowerProtect Cyber Recovery umfasst viele Komponenten, darunter einen oder mehrere Storage Vaults, die sich entweder in einer PowerProtect DD-On-Premise-Appliance (ehemals Data Domain) oder über den softwarebasierten Dell APEX Protection Storage for Public Cloud (ehemals DD Virtual Edition) in der Cloud befinden können. In beiden Fällen wird der Vault mit einem Air Gap betrieben, d. h., dass er von der Produktionsumgebung isoliert ist – potenziell mit einem physischen Air Gap bei der On-Premise-Umgebung und einem logischen Air Gap im Falle der Dell APEX-Umgebung. Dies macht es für böswillige AkteurInnen oder unbefugte NutzerInnen extrem schwierig, sich anzumelden und Sicherungskopien zu beschädigen.

PowerProtect Cyber Recovery umfasst außerdem CyberSense, eine vollständig automatisierte und integrierte intelligente Sicherheitsanalysen-Engine, die Daten, Dateien, Datenbanken und Images im Vault automatisch auf Anzeichen von Beschädigung durch einen Ransomwareangriff scannt. CyberSense bietet eine vollständige Inhaltsanalyse und nimmt Beobachtungen aus Dateien als Eingaben für sein auf künstlicher Intelligenz (KI) basierendes ML-Modell (maschinelles Lernen) auf. Die Lösung erkennt bösartige Aktivitäten, die Massenlöschungen, Verschlüsselung und andere verdächtige Änderungen in der Kerninfrastruktur (einschließlich Active Directory und DNS), den Nutzerdateien und den kritischen Produktionsdatenbanken umfassen, die auf Ransomware oder einen destruktiven Angriff hinweisen könnten. Wenn CyberSense Muster von Beschädigungen erkennt, wird eine Warnmeldung im PowerProtect Cyber Recovery-Dashboard erzeugt, die zusätzliche Informationen über die Größe und die Auswirkungen des Angriffs enthält.[1]

PowerProtect Cyber Recovery unterstützt Unternehmen dabei, Cyberangriffe abzuwehren, die Datenausfallsicherheit mit mehreren Kopien von Datenbackups an separaten Standorten zu verbessern, Ausfallzeiten zu reduzieren und die Business Continuity aufrechtzuerhalten. In diesem Bericht werden öffentlich verfügbare Daten verwendet, um wichtige Data-Protection-Funktionen aufzuzeigen. Außerdem werden unsere Ergebnisse einer Wettbewerbsanalyse von CyberSense vorgestellt.

Schützen sensibler Daten

Verschlüsseln Sie unveränderliche In-Flight-Daten während der Backupreplikation in physisch und logisch isolierten Vaults.

Erkennen der Beschädigung einer SQL Server-Seite

CyberSense hat eine Infektion gefunden, die von einer Konkurrenzlösung nicht erkannt wurde.

Identifizieren nicht beschädigter Sicherungskopien

CyberSense hat die neueste nicht infizierte Sicherungskopie für die Recovery identifiziert.

Sicherheit

Dell PowerProtect Cyber Recovery bietet mehrere Sicherheitsfunktionen, um kritische Daten vor Ransomware und anderen ausgefeilten Bedrohungen zu schützen. Diese verhindern, dass unbefugte NutzerInnen Zugriff auf vertrauliche Informationen erhalten, und ermöglichen eine schnelle Recovery, damit Unternehmen den normalen Betrieb fortsetzen können.

Die Funktionen und Merkmale von PowerProtect DD Appliances sind entscheidend für die Sicherheit, Integrität und Recovery, die PowerProtect Cyber Recovery-Lösungen bieten. Diese Merkmale umfassen:

1. **Unveränderbarkeit**
   Unveränderbare Daten können nicht geändert oder gelöscht, sondern nur geschrieben werden. DD-Systeme können unveränderbare Backups sowohl auf Produktionssystemen als auch im Cyber Vault schreiben. Wenn böswillige AkteurInnen also auf irgendeine Weise Zugriff auf das Backupsystem erhalten, können sie die vorhandenen geschützten Kopien nicht ändern, löschen oder kompromittieren.[2] Jede Sicherung, die das DD-System in der Produktionsumgebung erstellt, ist sofort unveränderbar und kann von der IT-Abteilung zur zusätzlichen Sicherheit in den Vault kopiert werden. Im nächsten Abschnitt dieses Berichts wird die Unveränderbarkeit näher untersucht.

2. **Retention Lock**
   DD Retention Lock macht Daten für einen vorab festgelegten Zeitraum unveränderbar. Sobald die Lösung Daten mit einer Aufbewahrungssperre versehen hat, können diese bis zum Ablauf der Sperrfrist weder von NutzerInnen noch vom System geändert, gelöscht oder modifiziert werden.[3]

   Retention Lock verfügt über Governance- und Compliancemodi. Im Compliancemodus können Kunden zahlreiche behördliche Standards erfüllen. Ein unabhängiger Drittanbieter hat bestätigt, dass DD Retention Lock die Storage-Anforderungen erfüllt, die in den SEC-Regeln 17a-4(f)(2) und 240.18a-6(e)(2) und der FINRA-Regel 4511(c) festgelegt sind.[4] Diese Funktion kann Unternehmen auch dabei unterstützen, die Anforderungen von FDA 21 CFR Part 11, Sarbanes-Oxley Act, IRS 98025 und 97-22, ISO-Norm 15489-1 und MoREQ2010 zu erfüllen.[5]

   Da AngreiferInnen versuchen könnten, Retention Lock durch Ändern der Systemzeit zu umgehen, wodurch die Lösung Dateien früher als erwartet löschen würde, verfügt DD über eine interne Sicherheitsuhr. Das System vergleicht regelmäßig die Zeiten der Sicherheitsuhr und Systemzeit. Wenn innerhalb eines Kalenderjahres eine kumulierte Abweichung von zwei Wochen zwischen den beiden Uhren auftritt, deaktiviert das System automatisch das DD-Dateisystem (DDFS), um den Zugriff auf Daten zu verhindern.[6]

3. **Verschlüsselung von In-Flight-Daten mit DDBoost**
   In-Flight-Daten können ein erhebliches Sicherheitsrisiko darstellen. DDBoost begrenzt die Menge der In-Flight-Daten, indem der Backupserver oder Anwendungsclient nur eindeutige Datensegmente anstelle aller Daten über das Netzwerk an die DD Appliance senden kann. Darüber hinaus können Unternehmen das DDBoost-Protokoll mit oder ohne Zertifikate für die Authentifizierung und Verschlüsselung von Daten verwenden. Zertifikate bieten eine höhere Sicherheit beim Datentransport. Mit der In-Flight-Verschlüsselung können Anwendungen In-Flight-Backup- oder Wiederherstellungsdaten über das LAN aus dem System verschlüsseln. Der Client kann Transport Layer Services (TLS) verwenden, um die Sitzung zwischen dem Client und dem System zu verschlüsseln.[7]

4. **Sicherheit des DD-Betriebssystems (DD OS)**
   Die DD-Sicherheitsfunktionen erstrecken sich auch auf das Betriebssystem. DD OS implementiert aus Sicherheitsgründen selbstdefinierte Zugriffskontrollen und Einschränkungen für die Bash-Shell. Im eingeschränkten Bash-Shell-Modus können NutzerInnen nur eine Reihe vordefinierter Befehle ausführen, die für ihre Rollen und Aufgaben erforderlich sind. DD OS verbessert die Datenintegrität, indem undefinierte Befehle blockiert werden, die nicht autorisierte oder unbeabsichtigte Änderungen am System vornehmen.[8]

5. **Sicherheit der rollenbasierten Zugriffskontrolle (RBAC) und des DD-Dateisystems (DDFS)**
   DD-Systeme verwenden mehrere Maßnahmen, um Dateien und Daten innerhalb des Dateisystems zu schützen. Zunächst bieten DD-Systeme eine rollenbasierte Zugriffskontrolle, mit der AdministratorInnen Rollen mit bestimmten Berechtigungen definieren und diesen Rollen NutzerInnen zuweisen können. Nur autorisierte NutzerInnen mit entsprechenden Berechtigungen können auf die Appliance und ihre Daten zugreifen. Dadurch wird sichergestellt, dass NutzerInnen nur auf die Funktionen und Daten zugreifen können, die sie für ihre Aufgaben benötigen, wodurch das Risiko eines unbefugten Zugriffs oder einer versehentlichen Offenlegung von Daten verringert wird.

   DDFS verwendet außerdem Hashing zur Überprüfung der Datenintegrität. Beim Hashing wird ein bestimmter Schlüssel oder eine Zeichenfolge in einen anderen Wert umgewandelt. Die Appliance speichert eindeutige Datenblöcke in logischen Storage-Containern und das Dateisystem hasht sowohl die Datenblöcke als auch die Container. Wenn das System Daten abruft, berechnet es den Hash-Wert der Daten neu, um ihn mit dem in DDFS gespeicherten Hash-Wert abzugleichen. Dadurch wird sichergestellt, dass die Daten nicht manipuliert oder beschädigt wurden.[9]

6. **Autorisierung über zwei Rollen**
   Wenn ein Unternehmen den Compliancemodus von DD Retention Lock aktiviert, bietet das DD-System zusätzliche administrative Sicherheit in Form einer dualen Anmeldung. Das bedeutet, dass sich sowohl der/die SystemadministratorIn als auch ein/e zweite/r autorisierte/r NutzerIn (z. B. der/die Sicherheitsbeauftragte) gemeinsam anmelden müssen. Der duale Anmeldemechanismus des Compliancemodus von DD Retention Lock fungiert als Schutz vor Aktionen, die die Integrität der gesperrten Dateien vor Ablauf der Aufbewahrungsfrist potenziell gefährden könnten.[10]

7. **Data Invulnerability Architecture**
   DD OS bietet End-to-End-Verifizierung, Fehlervermeidung und -eindämmung, kontinuierliche Fehlererkennung und Fehlerkorrektur sowie Wiederherstellbarkeit des Dateisystems, um Probleme mit der Datenintegrität zu vermeiden, die durch Hardware- und Softwarefehler verursacht werden. Wenn das DD-System Schreibanforderungen von der Backupsoftware empfängt, analysiert es zunächst ein Datensegment auf Redundanz, indem es den Fingerabdruck für das Datensegment berechnet und mit den im System gespeicherten Fingerabdrücken vergleicht. Es speichert nur eindeutige Datensegmente und deren Fingerabdrücke auf der Festplatte. Anschließend liest DD kontinuierlich Daten von der Festplatte zurück, berechnet den gelesenen Fingerabdruck neu und stellt sicher, dass er mit dem Fingerabdruck auf der Festplatte übereinstimmt. Das DD-System führt einen automatischen Fehlerkorrekturprozess durch, um beschädigte Daten zu rekonstruieren und in ihren korrekten Zustand zurückzuversetzen, wenn das System während dieses Prozesses eine Beschädigung feststellt (d. h. wenn das, was zurückgelesen wird, nicht mit dem übereinstimmt, was geschrieben wurde). Darüber hinaus trägt der Prozess zur automatischen Fehlerkorrektur dazu bei, das System vor anderen Änderungen zu schützen, die die Integrität der Plattform beeinträchtigen könnten.

Unveränderlichkeit*

Wenn Backups unveränderlich und somit schreibgeschützt sind, kann ein Unternehmen diesen Backups für die Recovery vertrauen. Betrieblich trägt die Unveränderlichkeit dazu bei, die Authentizität und Zuverlässigkeit der Daten aufrechtzuerhalten.

* Ziel der Produkte von Dell ist, Kunden bei ihren Bemühungen zum Schutz ihrer kritischen Daten zu unterstützen. Wie bei jedem elektronischen Produkt können auch bei Data-Protection-, Storage- und anderen Infrastrukturprodukten Sicherheitslücken auftreten. Es ist wichtig, dass Kunden Sicherheitsupdates installieren, sobald sie von Dell zur Verfügung gestellt werden.

Funktionsweise

DD-Systeme bieten Unveränderbarkeit bei der Speicherung von Daten mithilfe von MTrees. MTrees sind logische Partitionen des Dateisystems. Wenn eine Anwendung Daten in einen MTree schreibt, erstellt das DD-System mithilfe einer Funktion namens „Fast Copy" eine Point-in-Time-Kopie des ursprünglichen MTree in einem neuen MTree. Innerhalb des neuen MTree wendet DD Retention Lock an, um sicherzustellen, dass NutzerInnen und Prozesse den neuen MTree für die durch die Aufbewahrungsfrist definierte Dauer nicht löschen können. Der neue MTree ist eine unveränderliche Kopie der Daten und unabhängig vom ursprünglichen MTree.[11]

Die PowerProtect Cyber Recovery-Lösungen nutzen außerdem eine MTree-Replikation, um unveränderliche Datenkopien von einem Produktions-DD-System über das DDBoost-Protokoll auf ein anderes DD-System im Vault zu kopieren.[12] Bei der anfänglichen Synchronisation zwischen den beiden DDs kopiert die Lösung alle Daten auf die Vault-DD. Bei jeder nachfolgenden Synchronisation werden nur neue und geänderte Datensegmente kopiert. CyberSense, auf das wir später in diesem Bericht eingehen werden, scannt alle unveränderbaren Kopien im Vault auf potenzielle Beschädigungen.

Ansätze für Unveränderbarkeit

Es kommt zwar selten vor, dass unveränderbare Backups gelöscht werden müssen, jedoch kann dieser Fall eintreten. Unternehmen können möglicherweise Kapazitäts- und damit verbundene Kostenprobleme bekommen, wenn sie unveränderbare Backups ansammeln, die sie nicht löschen können. Die Speicherung von Backups kann erhebliche Kapazitäten erfordern, was zusätzlich zu den anfänglichen Hardwareinvestitionen laufende Betriebs-, Verwaltungs- und Überwachungskosten verursacht. Das regelmäßige Löschen unveränderlicher Backups kann zur Lösung dieser Probleme beitragen.

Wie bereits erwähnt, erreicht Dell PowerProtect Cyber Recovery Unveränderbarkeit durch die Nutzung von Retention Lock und anderen Tools. Retention Lock bietet eine gewisse Flexibilität, da die beiden Modi „Compliance" und „Governance" geringfügige Änderungen hinsichtlich der Implementierung der Unveränderbarkeit durch Kunden ermöglichen. Unveränderbarkeit bedeutet, dass NutzerInnen oder böswillige AkteurInnen Backups nicht löschen können. In bestimmten Fällen, z. B. bei Problemen mit der Speicherkapazität, können Kunden diese jedoch mit PowerProtect Cyber Recovery im Governancemodus von Retention Lock löschen.

Wie schneiden ähnliche Angebote anderer Unternehmen im Vergleich zu PowerProtect Cyber Recovery ab? Wir haben uns öffentlich verfügbare Informationen zu Cohesity Cyber Recovery, Veeam, Rubrik und Veritas NetBackup angesehen. Mit Ausnahme von Cohesity Cyber Recovery können die Lösungen entweder On-Premise oder extern bereitgestellt werden (Cohesity ist eine cloudbasierte Lösung, die von AWS unterstützt wird). Die Dokumentation der vier Lösungen behauptet, Unveränderlichkeit zu bieten, aber Rubrik und NetBackup unterscheiden sich merklich von PowerProtect Cyber Recovery.

Bei Rubrik können AdministratorInnen Backups löschen, jedoch nicht von der Client-Seite aus und nur mit bestimmten Kontrollen. Darüber hinaus sind alle Schreibvorgänge „out-of-place", d. h., neue Schreibvorgänge berühren niemals zuvor geschriebene Daten.[13]

Trotz der Unveränderbarkeit können AdministratorInnen oder böswillige AkteurInnen die Sperre für Backups in einem WORM-fähigen NetBackup-Storage aufheben. Anschließend könnten sie das Image mit dem Befehl „bpexpdate" löschen.[14]

Isolierung

Datenisolierung bezieht sich auf die Trennung und eingeschränkte Zugänglichkeit von Daten, ermöglicht durch Barrieren oder Grenzen, die einen unbefugten Zugriff zu verhindern. Für die Isolierung werden temporäre Netzwerkverbindungen anstelle von persistenten Verbindungen verwendet.

Die Datenisolierung trägt dazu bei, dass kritische Daten nicht mit einem infizierten Netzwerk verbunden bleiben, in dem böswillige AkteurInnen versuchen könnten, Konfigurationen zu modifizieren, Daten zu löschen, Richtlinien zu ändern oder den Netzwerkverkehr auf Nutzerzugangsdaten zu durchsuchen. Mithilfe einer Isolierung kann außerdem die Angriffsfläche verkleinert werden, sodass böswillige AkteurInnen weniger Möglichkeiten haben, Zugriff und Kontrolle zu erhalten. Darüber hinaus können Unternehmen den Zugriff auf autorisierte MitarbeiterInnen einschränken und so verhindern, dass unbefugte NutzerInnen Daten überschreiben.

Zusätzlich zu den erwähnten Funktionen kann PowerProtect Cyber Recovery sowohl eine physische als auch eine logische Isolierung in Form von betrieblichen Air Gaps bieten, um Daten zu schützen. PowerProtect Cyber Recovery kann sowohl einen physischen Air Gap verwenden, bei dem die Backupdaten physisch vom Produktionsnetzwerk getrennt und an einem isolierten Ort gespeichert werden, als auch einen logischen Air Gap, der auf Netzwerkzugriffskontrollen angewiesen ist, um die logisch separierten Backupkopien von der Produktionsumgebung zu trennen. Beide Arten von Air Gaps sind wertvoll, da ein logischer Air Gap allein nicht verhindern kann, dass interne NutzerInnen mit Netzwerkzugriff auf den Vault auf die Daten zugreifen und diese kompromittieren.

Eine physisch isolierte PowerProtect DD-On-Premise-Lösung kann als Vault fungieren, in dem NutzerInnen oder Systeme aus der Produktionsumgebung nicht auf die Komponenten zugreifen können und der Vault physisch vom Produktionsnetzwerk getrennt ist.[15] Durch die Beseitigung des Zugriffs auf die Recovery-Umgebung über das Produktionsnetzwerk kann ein Unternehmen seine Angriffsfläche verkleinern. Wie bereits erwähnt, erfordert der Zugriff auf die isolierten Daten separate Sicherheitszugangsdaten sowie eine Multifaktor-Authentifizierung (MFA).[16]

Ansätze zur Isolierung

Gartner stellt fest: „Isolierte Wiederherstellungsumgebungen (IREs) mit unveränderbaren Datenspeichern (IDVs) bieten ein Höchstmaß an Sicherheit und Recovery gegenüber Insiderbedrohungen, Ransomware und anderen Formen des Hackings.“[17] Außerdem wird darauf hingewiesen, „eine IRE mit einem IDV herkömmliche Backup- und Disaster-Recovery-Systeme (DR) nicht ersetzt, sondern ergänzt, indem sie eine tertiäre unveränderbare Backupkopie in einer IRE bereitstellt, die mit allen Tools, Prozessen und Ressourcen zur Wiederherstellung betroffener Systeme ausgestattet ist.“[18]

Bei der Durchsicht öffentlich verfügbarer Informationen zu den Lösungen von Cohesity, Veeam, Rubrik und Veritas haben wir festgestellt, dass jede dieser Lösungen einen zumindest leicht unterschiedlichen Ansatz für IRE als PowerProtect Cyber Recovery verfolgt. Mit der Dell Lösung können Kunden ihre DD Vaults physisch oder logisch von der Produktion isolieren, um die Steuerungs- und Datenebenen der Produktion von den Vaults getrennt zu halten. Darüber hinaus automatisiert PowerProtect Cyber Recovery Air Gaps, was nicht alle anderen Lösungen können.

In der Dokumentation wird Folgendes angegeben:

- Cohesity Cyber Recovery bietet nur einen dynamischen automatisierten logischen Air Gap für seinen AWS-basierten FortKnox-Vault.[19]
- Veeam unterstützt einen logischen Air Gap für Public- und Private-Cloud-Anbieter über Veeam Cloud Connect, dieser ist jedoch nicht automatisiert. Veeam bietet außerdem Veeam Hardening Repository an, das als On-Premise-Vault für die Lösung fungiert und von Unternehmen so konfiguriert werden kann, dass ein physischer Air Gap vorhanden ist.[20]
- Rubrik bietet keinen automatisierten Air Gap für Rubrik Cloud Vault, aber Kunden können einen logischen Air Gap über eine Drittanbieterpartnerschaft mit Microsoft hinzufügen.[21]
- NetBackup-Kunden müssen manuell einen logischen Air Gap aktivieren und können mit einer On-Premise- oder externen Lösung einen physischen Air Gap erstellen.[22]

Funktionsweise

Abbildung 1 zeigt die Netzwerkpfade des isolierten Cyber Recovery Vault. Beachten Sie, dass der Vault keinen Management- oder Kontrollpfad zur Produktionsumgebung hat, um die Angriffsfläche zu reduzieren.

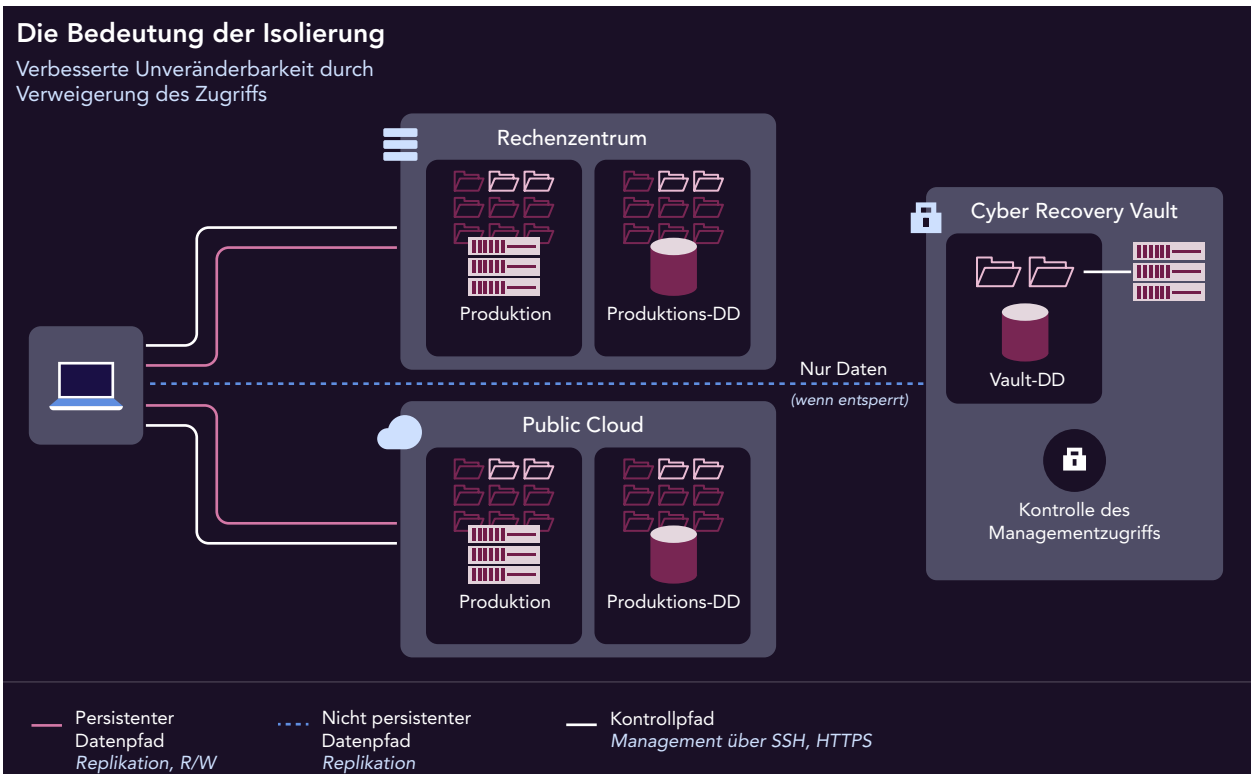


Abbildung 1: Allgemeine Daten- und Kontrollpfadarchitektur des Cyber Recovery Vault. Quelle: Principled Technologies

Die einzige erforderliche Verbindung für den Cyber Recovery Vault ist ein Datenpfad für die regelmäßige Datensynchronisation. Bei der Synchronisation nimmt die Cyber Recovery-Lösung Daten in kurzen, Policy-gesteuerten Intervallen für die Replikation auf.[23] Im PowerProtect Cyber Recovery Solution Guide heißt es: „Die Basisarchitektur der Cyber Recovery-Lösung besteht aus einem Paar von PowerProtect DD-Systemen und dem Cyber Recovery-Managementhost. In dieser Basiskonfiguration aktiviert und deaktiviert die auf dem Managementhost ausgeführte Cyber Recovery-Software die Replikations-Ethernet-Schnittstelle zusammen mit Replikationskontexten auf dem PowerProtect DD-System im Cyber Recovery Vault, um den Datenfluss von der Produktionsumgebung zur Vault-Umgebung zu steuern."[24] Dell schlägt zusätzliche Möglichkeiten vor, wie Unternehmen Datenpfade sichern und isolieren können. In unseren Tests haben wir beobachtet, dass Cyber Recovery den Vault während und nach der Replikation entsperrt und sperrt.

Für die physische Implementierung des Vault empfiehlt Dell die „Installation der Cyber Recovery Vault-Geräte in einem dedizierten Raum oder Gehäuse mit physischen Zugriffskontrollen. Dieser gesicherte Raum sollte über eine Liste mit eingeschränktem Zugriff verfügen, die eine Schlüsselausgabe oder einen Zugang durch zwei Personen erfordert. Die Eingänge zum Käfig oder Raum sowie die Geräte sollten videoüberwacht werden. Für maximale Sicherheit darf die Cyber Recovery-Software nur durch physischen Zugriff auf den Cyber Recovery-Managementserver und eine zugehörige Tastatur und Maus zugänglich sein."[25]

Durch die Trennung der Management- und Kontrollpfade unterscheiden sich die physischen und logischen Air-Gap-Isolierungsoptionen in Cyber Recovery von anderen Lösungen. Einige Lösungen ermöglichen den Zugriff auf ihre Vault-Daten über eine Schnittstelle in der Produktionsumgebung. Dadurch befinden sich die Vault-Daten auf derselben Angriffsfläche wie die Produktionsdaten, sodass böswillige AkteurInnen möglicherweise mit kompromittierten Zugangsdaten auf Backupkopien zugreifen können.

CyberSense

Für einen guten Schutz Ihrer Daten ist eine umfassende Strategie erforderlich, die Sicherheit auf jeder Ebene bietet. Trotz aller Funktionen für automatische Fehlerkorrektur, Sicherheit, Unveränderlichkeit und Isolierung einer Dell PowerProtect Cyber Recovery-Lösung könnten weniger offensichtliche Angriffe dennoch tiefer in eine Unternehmensinfrastruktur eindringen, z. B. auf Datenbackupebene, und potenziell unbemerkt bleiben, bis Produktionsdaten oder eine gesamte Nutzergruppe kompromittiert wurden. Dell PowerProtect Cyber Recovery-Lösungen bieten eine letzte Verteidigungslinie gegen Cyberangriffe und einen effizienten Ansatz, um die Recovery über CyberSense zu beschleunigen. CyberSense ist eine Analyse-Engine, die KI-basierte ML-Analysealgorithmen verwendet, um die Integrität von Backups im Vault und den Nutzerinhalt der Dateien innerhalb der Backups zu scannen und validieren.

CyberSense wird innerhalb des Vault ausgeführt und ist von der Produktionsumgebung isoliert. Es überwacht Dateien, VM-Images und Datenbanken innerhalb des Vault, um durch Analyse der Datenintegrität festzustellen, ob ein Angriff stattgefunden hat. Sobald die Cyber Recovery-Lösung Backupkopien in den Vault repliziert und die Retention Lock-Funktion anwendet, scannt CyberSense die Kopien automatisch und erstellt Point-in-Time-Beobachtungen von Dateien, Datenbanken und Core-Infrastruktur. Die Analyse-Engine scannt den gesamten Inhalt von Dateien und jeder Datenbankseite – nicht nur Metadaten. Während andere Lösungen nach Änderungen an Datenschwellenwerten oder Metadaten suchen, überprüft CyberSense den Inhalt von Dateien, um die Datenintegrität zu validieren. Mit diesen Beobachtungen kann CyberSense verfolgen, wie sich Dateien und Datenbanken im Laufe der Zeit verändern, und viele fortgeschrittene Arten versteckter Angriffe aufdecken. Anschließend generiert CyberSense Analysen, die Muster von Beschädigungen erkennen, die auf böswillige Aktivitäten hinweisen können, darunter Verschlüsselung, Löschung, Erstellung oder Verschleierung von Dateien und vieles mehr.[26] Andere Lösungen übertragen die Analyse in die Cloud, wodurch sich die Angriffsfläche potenziell vergrößert. Unternehmen können CyberSense hingegen vor Ort oder in einer der vielen Cloud-Optionen ausführen, die Cyber Recovery unterstützt.

CyberSense kombiniert über 200 Analysen mit Datenbeobachtungen, die mit zunehmender Beobachtungsdauer immer nützlicher werden. Der ML-Algorithmus verwendet Informationen über Tausende von Malware-Infektionen, um ungewöhnliche Verhaltensmuster zu finden und Nutzeraktivitäten von Ransomware zu unterscheiden. Gleichzeitig werden falsch positive und negative Ergebnisse minimiert. Der Algorithmus wird durch kontinuierliche Forschung mit neuen Informationen, beispielsweise zu Angriffsvarianten, aktualisiert. Darüber hinaus erhält der ML-Algorithmus Updates auf der Grundlage von realen Daten bestehender CyberSense-Kunden.[27]

Zusätzlich unterstützt CyberSense die Indexierung von Daten in gängigen Festplattenbackupformaten von Dell, IBM, CommVault und Veritas.[28] Durch die Unterstützung von Backupformaten anderer Anbieter zeigt Dell seine Bereitschaft, auf die individuellen Anforderungen seiner Kunden im Bereich Datenbackups einzugehen.

Wir haben die ML-gesteuerte intelligente Analysesoftware von zwei gebrauchsfertigen Lösungen für Unternehmensdatensicherheit und Cyber-Recovery getestet: CyberSense für Dell PowerProtect Cyber Recovery auf einem Dell PowerStore™ 7000T und ein ähnlich funktionierendes Tool aus der Datenmanagementplattform eines Mitbewerbers („Anbieter X“) für ein Gerät ähnlicher Größe.

Testbeschreibung

Wir haben alle Tests remote durchgeführt und hatten die volle Kontrolle über die Testumgebungen sowie uneingeschränkten Zugriff darauf. Sowohl die Dell Lösung (einschließlich CyberSense, der PowerProtect Data Manager-Backupanwendung, APEX Protection Storage (früher bekannt als DD Virtual Edition) und der PowerProtect Cyber Recovery-Lösung) als auch die Lösung von Anbieter X befanden sich in einem externen Rechenzentrumslabor.

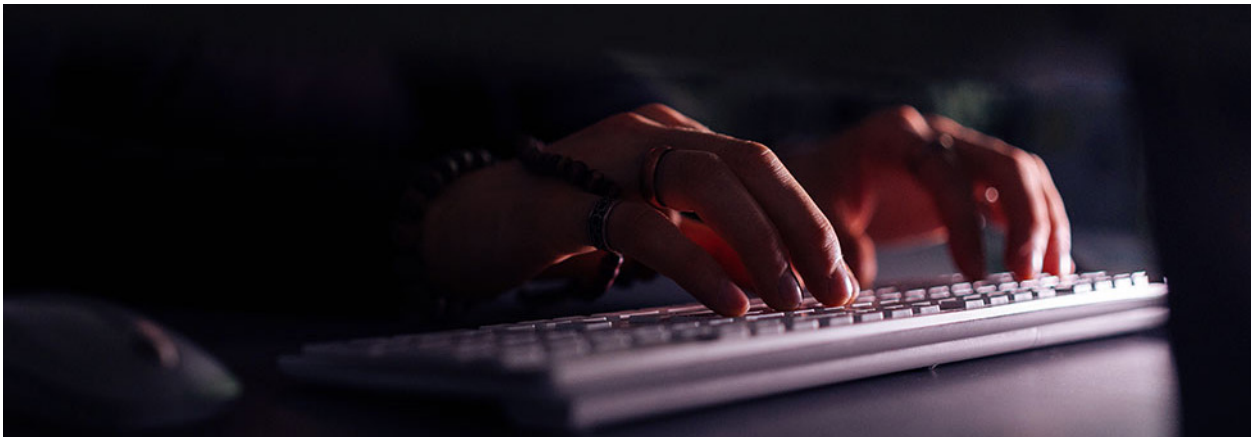
Auf beiden Lösungen haben wir drei skriptbasierte Szenarien mit bösartigen Ereignissen ausgeführt, die auf Backups abzielten:

Abbildung 2: Unsere Testszenarien. Quelle: Principled Technologies

Bei beiden Lösungen folgten die ersten beiden Szenarien demselben allgemeinen Verfahren. Zunächst haben wir ein vollständiges Backup aller sauberen VMs auf den Storage-Appliances von Dell PowerProtect Data Manager und Vendor X erstellt, inkrementelle Backups für das Scannen erstellt und überprüft, dass die Ziellösung keine Bedrohung erkannt hat. Dadurch erhielten wir einen Baseline-Satz von Backups, auf denen wir die Angriffsskripte ausführen konnten.

Als Nächstes führten wir das Ransomware-Simulationsskript auf vier VMs mit verschiedenen Betriebssystemen und Anwendungstypen aus, erstellten neue inkrementelle Backups auf dem Zielgerät und überprüften, ob die Zielanalysesoftware die Verschlüsselungsbedrohung erkannt hat.

Für das dritte Szenario (Infektion einer SQL Server-Seite) folgten wir einem ähnlichen Verfahren wie in den beiden anderen Szenarien, konzentrierten uns jedoch auf SQL-VMs und verwendeten anstelle eines Verschlüsselungsskripts ein Skript zur Beschädigung von Seiten. Wir haben das Skript auf einer einzelnen VM ausgeführt.



Unsere Ergebnisse

Szenario 1: Erkennen verschlüsselter Dateien mit verschleierten Dateinamen

In diesem Szenario wurde ein bösartiges Ereignis simuliert, bei dem Dateien verschlüsselt und ihre Namen verschleiert wurden, wodurch neben dem Inhalt auch die Metadaten der Datei geändert wurden. Diese Art von Angriff wird in der Regel als Ransomware bezeichnet, ein Sicherheitsereignis, bei dem bösartige Software den Zugriff auf Computersysteme blockiert, bis die EigentümerInnen oder NutzerInnen des Systems einen vorab festgelegten Betrag zahlen. Laut der US-amerikanischen Cybersecurity and Infrastructure Security Agency (CISA) haben sich die wirtschaftlichen und rufschädigenden Auswirkungen von Ransomware und Datenerpressung für Unternehmen jeder Größe während der anfänglichen Unterbrechung und manchmal auch der erweiterten Recovery als schwierig und kostspielig erwiesen.[29] Die Nutzung einer intelligenten Analysesoftware zur Erkennung von Verschlüsselungen in Backups kann die Data-Protection-Strategie eines Unternehmens stärken, wertvolle und vertrauliche Informationen schützen sowie potenzielle kostspielige Ausfallzeiten aufgrund von Cyberangriffen reduzieren.

In unseren Tests haben beide intelligente Analyseanwendungen die verschlüsselten Dateien mit geänderten Dateinamen erkannt. Die Lösung von Anbieter X benötigte eine Baseline von 15 Backups, bevor Infektionen erkannt wurden (ein vollständiges Backup und 14 inkrementelle Backups), während CyberSense Infektionen nach nur einem vollständigen Backup erkannte, was bedeutet, dass die Lösung von Anbieter X im Vergleich zu CyberSense 14 zusätzliche Backups erforderte.

Als uns die Lösung von Anbieter X auf die verdächtige Aktivität aufmerksam machte, wies sie lediglich darauf hin, dass einige Dateien entfernt und eine gleiche Anzahl von Dateien hinzugefügt wurden. Dies stellte aufgrund der Entropiebewertung der Sicherung eine verdächtige Aktivität dar.[30] Die Lösung von Anbieter X gab nicht an, dass die Dateien verschlüsselt worden waren oder dass sich die Dateinamen geändert hatten. Im Gegensatz dazu warnte uns Cyber Recovery mit CyberSense, dass Dateinamen verschlüsselt und verschleiert worden waren.

Die Ergebnisse für Anbieter X können auf ein falsch positives Ergebnis hinweisen. Mit anderen Worten: Wenn wir davon ausgehen, dass ein Unternehmen mit der Lösung von Anbieter X täglich Backups durchführt, könnten 14 Tage lang infizierte Dateien aufgenommen worden sein, bevor die Anomalie erkannt wurde. Im Gegensatz dazu benötigte CyberSense nur ein Baseline-Backup, um mit intelligenten Informationen über die Infektion und deren Details zu warnen. Die Recovery mit Cyber Recovery erfolgt in diesem Stadium unseres Beispiels aus dem isolierten Vault, sodass das Unternehmen sicher sein kann, dass das Produktionsnetzwerk nicht den 14 infizierten Backups ausgesetzt war, wie es bei der Lösung von Anbieter X der Fall gewesen wäre.

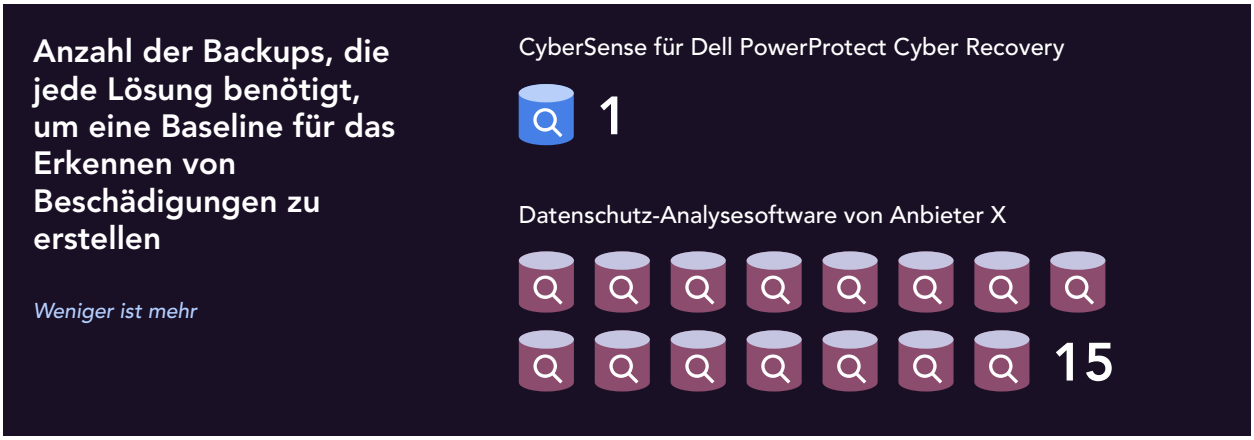


Abbildung 3: Die Anzahl der Backups, die jede Lösung benötigt, um eine Baseline für das Erkennen von Beschädigungen zu erstellen.
Quelle: Principled Technologies

Szenario 2: Erkennen verschlüsselter Dateien mit ursprünglichen Dateinamen

Dieses Szenario ähnelte dem ersten Szenario, jedoch behielt das Skript die ursprünglichen Dateinamen der verschlüsselten Dateien bei. Diese Änderung hatte keine Auswirkungen auf die Metadaten der Dateien, sondern nur auf die Dateien selbst. Eine solche Vorgehensweise könnte auf eine Timebomb-Ransomware hindeuten, bei der der Angriff zunächst eine Zeit lang inaktiv bleibt, bevor er aktiviert wird. Timebomb-Ransomware kann der Erkennung entgehen und Backups angreifen, sodass die infizierten Backups unbrauchbar werden, wenn das Unternehmen sie benötigt.[31] Ohne Änderungen an den Metadaten kann die Datei oberflächlich betrachtet als nicht infiziert erscheinen, wodurch der ruhende Angriff verborgen bleibt.

In unseren Tests haben beide intelligente Analyseanwendungen die verschlüsselten Dateien erkannt. Auch hier benötigte die Lösung von Anbieter X eine Baseline von 15 Backups, einschließlich 14 inkrementellen Backups, bevor sie eine Anomalie erkennen konnte. CyberSense benötigte eine Baseline von nur einem vollständigen Backup, bevor eine Anomalie erkannt wurde.

Wie im ersten Szenario warnte uns die Lösung von Anbieter X lediglich, dass sich viele Dateien geändert hatten, was aufgrund der Entropiebewertung der Sicherung verdächtig war. Es gab keinen Hinweis darauf, dass die Dateien verschlüsselt worden waren, während Cyber Recovery mit CyberSense uns dies mitteilte. Die Erkennung von Beschädigungen auf diese Weise bedeutet, dass CyberSense den Inhalt der Dateien und nicht nur die oberflächlichen Metadaten überprüft. Diese Art von Scan bietet eine zusätzliche Sicherheitsebene für Ihre Backups und damit für Ihre gesamte digitale Infrastruktur oder Ihren gesamten digitalen Bestand. Man könnte sagen, dass CyberSense eine „echte" intelligente Analyseanwendung ist. Darüber hinaus können Unternehmen mit CyberSense Beschädigungen möglicherweise früher erkennen, da die Lösung deutlich weniger Backups benötigt, um eine Baseline zu erstellen. Je nach Backupzeitplan eines Unternehmens kann dies viele Tage früher sein.

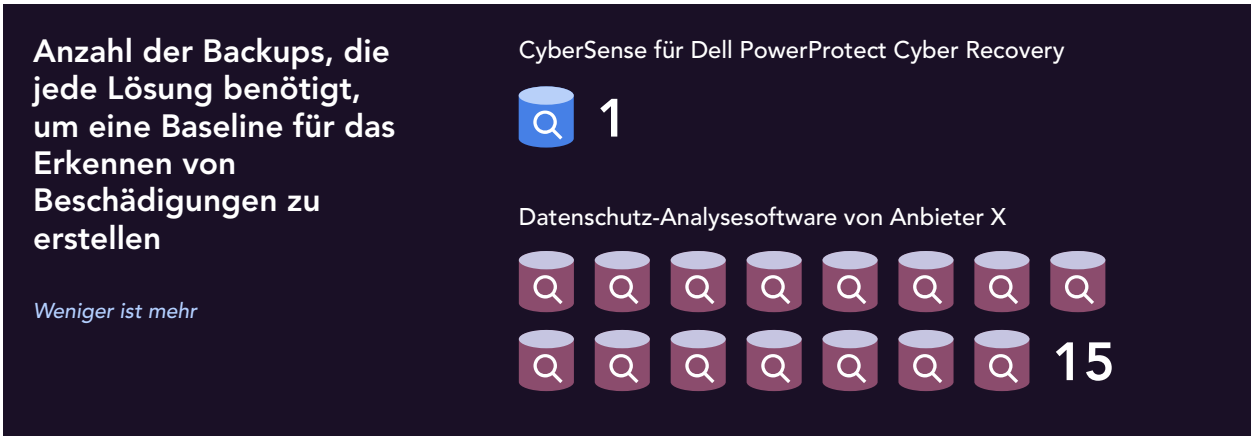


Abbildung 4: Die Anzahl der Backups, die jede Lösung benötigt, um Beschädigungen zu erkennen. Quelle: Principled Technologies

Szenario 3: Erkennen der Beschädigung einer SQL Server-Seite

In diesem Szenario wurde ein bösartiges Ereignis simuliert, bei dem eine SQL Server-Seite beschädigt wurde. In SQL Server ist die Seite die grundlegende Einheit des Daten-Storage, und die Datenbank liest oder schreibt ganze Datenseiten.[32] Auch diese Änderung hatte keine Auswirkungen auf Metadaten, sondern nur auf die Dateien selbst. Diese Art von Angriff ist allgemein als SQL-Injektion bekannt, bei der Angreifer SQL-datenbasierte Anwendungen angreifen, indem sie über Webseiteneingaben bösartigen Code in SQL-Anweisungen einschleusen.[33] Selbst wenn sie infiziert sind, werden Datenbanken möglicherweise weiterhin ausgeführt. Neben Datendiebstahl kann die Beschädigung von SQL Server-Seiten zu Datenintegritätsproblemen, Datenverlusten und Störungen der Datenbankfunktionalität führen. Dies kann den Ruf eines Unternehmens schädigen, Betriebsabläufe stören, zu finanziellen Verlusten führen und sogar rechtliche Konsequenzen nach sich ziehen.

Obwohl CyberSense und die Lösung von Anbieter X die Verschlüsselung in den ersten beiden Szenarien erkannt haben, war nur CyberSense in der Lage, tief genug zu scannen, um die Beschädigung der SQL Server-Seite im dritten Szenario zu erkennen. Dies zeigt, dass beide Lösungen zwar auf einigen Ebenen ähnliche Erkennungsfähigkeiten bieten, CyberSense jedoch eine tiefere Untersuchung von Backups für potenziell geschäftskritische SQL Server-basierte Anwendungen ermöglicht. Auf diese Weise bietet CyberSense eine zusätzliche Ebene der Sicherheitsresilienz mit tieferen Scans und umfassenderem Schutz.

SQL Server ist die Grundlage für viele Anwendungen in der Finanz-, Einzelhandels-, Gesundheits- und anderen Branchen. Da SQL Server als Backend der Entwicklungsarchitektur fungieren kann, kann ein Angriff auf SQL Server zu Ausfallzeiten, Betriebsunterbrechungen und potenziell zu einer Gefährdung der mit diesen Anwendungen erzielten Einnahmen führen.

Wiederherstellen mit Dell PowerProtect Cyber Recovery

Die Dell Strategie für Ausfallsicherheit bei Cyberangriffen bietet ein breites Angebot an Recovery-Funktionen. Diese Recovery-Optionen umfassen branchenübliche Funktionen wie sofortigen Zugriff oder herkömmliche Wiederherstellung aus unveränderbaren Backups, die in der Produktion aufbewahrt werden. Darüber hinaus ermöglicht Dell einzigartige Recovery-Funktionen mit der PowerProtect Cyber Recovery-Lösung. Da PowerProtect Cyber Recovery Kopien isoliert aufbewahrt und mit CyberSense auf Integrität überprüft, können Unternehmen unmittelbar nach einem Angriff auf die Kopien zugreifen und sie für eine schrittweise Recovery oder sofortige Wiederherstellungen auf alternativen Recovery-Plattformen, wie z. B. Reinräumen, verwenden.

Vergleichen Sie diesen unmittelbaren Anwendungsfall mit einem Unternehmen, das nur auf Daten in der Produktion oder in der Public Cloud zugreifen kann. Das Unternehmen kann erst dann sicher auf die im kompromittierten Bereich gespeicherten Daten zugreifen, wenn es die Ursache ermittelt und behoben, die Persistenz der Angreifer unterbunden, forensische Images für Versicherer und die Rechtsabteilung erstellt, die Daten erneut gescannt und über eine ausreichende Infrastruktur (AD, DNS) für den Zugriff auf die Backup-Infrastruktur verfügt. Dieser Prozess kann je nach Umfang und Komplexität des Angriffs Tage oder Wochen dauern.

Funktionsweise

Während der normalen Produktion erstellt PowerProtect Cyber Recovery automatisch Wiederherstellungspunkte für die Recovery und Sicherheitsanalysen. Im Falle eines Cyberangriffs nutzt Cyber Recovery seine automatisierten Wiederherstellungs- und Recovery-Verfahren sowie diese Wiederherstellungspunkte, um geschäftskritische Systeme wieder online zu bringen. CyberSense und forensische Berichte helfen Cybersicherheits- und Recovery-Teams, die Auswirkungen des Angriffs zu diagnostizieren. Sobald die Produktionsumgebung bereinigt und für die Recovery bereit ist, stellt Cyber Recovery die Tools und Technologien für die eigentliche Daten-Recovery bereit.

Nach einem Cyberangriff kommen mehrere Data-Protection-Metriken zum Einsatz, um die Geschwindigkeit der Recovery (die Cyber Recovery Time bzw. CRT) und den Zeitpunkt zu bestimmen, zu dem NutzerInnen nach einem zerstörerischen Angriff zurückkehren können (der Cyber Recovery Point bzw. CRP). Für eine Cyber Recovery-Lösung umfassen diese Metriken Folgendes:

- **Ziel für die Erkennung einer Vernichtung (Destruction Detection Objective, DDO)** – Hierbei handelt es sich um ein rollierendes Fenster, das auf der Zeitspanne zwischen einem Angriff und der Erkennung des Angriffs basiert. Analysen und andere Cyber Recovery-Mechanismen müssen innerhalb dieses Zeitraums funktionieren.
- **Ziel für die Bewertung einer Vernichtung (Destruction Assessment Objective, DAO)** – Dies ist die Zeit, die dem Cybersicherheitsteam nach einem Angriff zur Verfügung steht, um das Ausmaß des Schadens und mögliche Reaktionen zu ermitteln.
- **Cyber Recovery-Synchronisierungsintervall** – Dies ist die Häufigkeit, mit der die Cyber Recovery-Lösung Daten aus der Produktionsumgebung in den Vault kopiert. Das Timing basiert auf einem zuvor festgelegten Recovery Point Objective (RPO) für die Lösung. Der Zeitraum für die Aufbewahrung der Kopien variiert je nach Lösung, beträgt jedoch in der Regel zwischen einer Woche und einem Monat.
- **Anzahl der Cyber-Recovery-Datenkopien** – Dies ist die Anzahl der Datenkopien, die im Cyber Recovery-Vault gespeichert sind. In Kombination mit dem Synchronisierungsintervall bietet diese Metrik einen groben Anhaltspunkt dafür, wie weit in der Vergangenheit ein Unternehmen Daten wiederherstellen kann. Beispielsweise ermöglichen sieben Kopien in Kombination mit einem 24-Stunden-Intervall NutzerInnen die Wiederherstellung von Daten, die bis zu einer Woche alt sind.

Zusätzlich zu den Recovery-Anforderungen kann die Art der Daten, die die Lösung schützt, bei der Festlegung des Datensynchronisierungsintervalls und der Aufbewahrungsdauer hilfreich sein. Gemäß dem Cyber Recovery Solution Guide können NutzerInnen für eine größtmögliche Flexibilität bei der Recovery die von der Lösung geschützten Daten in einen der folgenden Backupstreams kategorisieren:[34]

- Binäre und ausführbare Backups, einschließlich grundlegender Betriebssystemverteilungen und Anwendungs-Builds
- Vollständige Anwendungs- und Dateisystem-Backups, einschließlich Images und anwendungsspezifischer Daten

Diese separaten Backupstreams führen zu zwei verschiedenen Recovery-Strategien:

1. **Wiederherstellung von Daten und Anwendungsbinärdateien im Cyber Recovery Vault:** Die Lösung identifiziert nutzbare Wiederherstellungspunkte sowie Malware und deren Speicherort und entscheidet, ob die Malware aus dem Backup-Image bereinigt oder mithilfe von Cyber Recovery Vault-Kopien neu erstellt werden soll. Nach dem Anwenden von Sicherheitspatches stellt die Lösung Daten mithilfe des DR-Runbooks für die Anwendung auf einem Recovery-Host wieder her und bestimmt dann, ob der Recovery-Prozess die Auswirkungen der Malware beseitigt hat. Anschließend führt sie einen Testlauf der Anwendung mithilfe von Vault Compute durch und bereinigt die Produktionsumgebung oder erstellt ein neues Image davon. Schließlich verbindet Cyber Recovery den Recovery-Host mit der Produktion und kopiert die Anwendung und Daten zurück in die Produktionsumgebung. In Abbildung 5 ist dieser Prozess dargestellt.

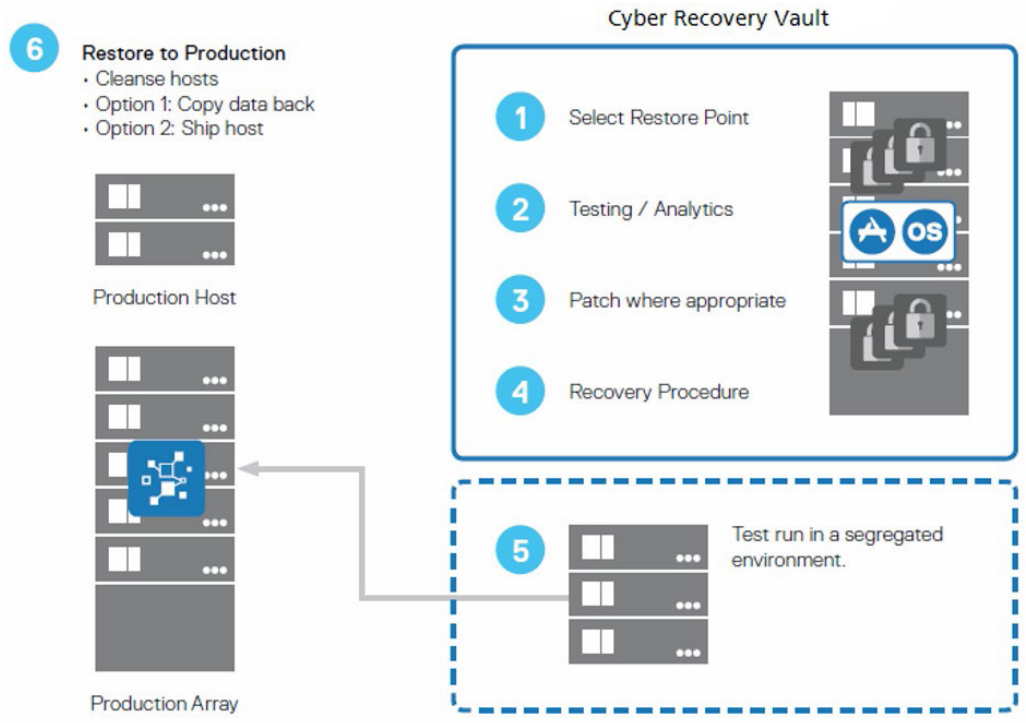


Abbildung 5: Der Prozess für die Wiederherstellung von Daten- und Anwendungsbinärdateien. Quelle: Dell Technologies.[35]

2. **Vollständige Neuerstellung aus dem Cyber Recovery Vault:**
   Bei diesem Ansatz formatiert die Cyber Recovery-Lösung die Produktionssysteme neu, basierend auf dem Ausmaß der Schäden, die bei der forensischen Untersuchung während der Incident Response ermittelt wurden. Anschließend erstellt die Lösung Binärdateien über Kopien im Cyber Recovery Vault neu und wendet verfügbare Sicherheitspatches an. Zuletzt stellt sie mithilfe der zugehörigen DR-Runbooks für die Anwendung die entsprechenden Kopien von Anwendungen, Daten und Konfigurationsdateien in der Produktionsumgebung wieder her. In Abbildung 6 ist dieser Prozess dargestellt.

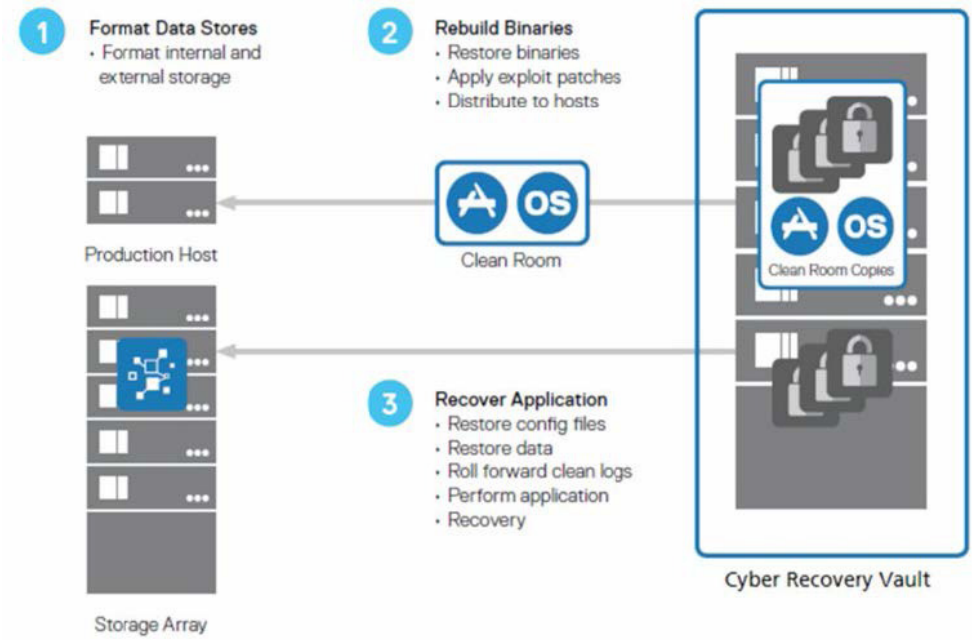


Abbildung 6: Der Prozess für die vollständige Neuerstellung aus dem Cyber Recovery Vault. Quelle: Dell Technologies.[36]

Die Cyber Recovery-Lösungen umfassen physische oder virtuelle Recovery-Hosts (oder beides), die die Cyber Recovery-Software für die Recovery verwenden kann. Diese Hosts umfassen sowohl einen Recovery-Server für Backupanwendungen, d. h. einen designierten Server, auf dem die Backupanwendung und der Backupanwendungskatalog wiederhergestellt werden, als auch einen Recovery-Server für Anwendungen. Unternehmen können je nach Recovery-Anforderungen der Lösung mehrere Server bereitstellen. Die Cyber Recovery-Software kann Sandbox-Datenkopien (eine Testumgebung zum sicheren Ausführen neuer oder ungetesteter Software) für jeden Host verfügbar machen, um Daten innerhalb des Vault wiederherzustellen, z. B. Dateisystemdaten, IBM-, Commvault- und Veritas-Sicherungsdaten oder Daten, die durch Dell NetWorker, Dell Avamar, eine Dell PowerProtect DP Series Appliance oder Dell PowerProtect Data Manager-Software geschützt sind. Nach der Wiederherstellung einer Backupanwendung im Vault kann die Lösung diese Daten auf zusätzlichen Recovery-Hosts im Vault wiederherstellen.

Unternehmen dimensionieren den Recovery-Server für Backupanwendungen im Voraus, sodass NutzerInnen alle Backupanwendungen wiederherstellen können, die von der Cyber Recovery-Lösung geschützt werden. In ähnlicher Weise ist der Recovery-Server für Anwendungen ein designierter Server, auf dem die Lösung Anwendungen wiederherstellt. Bei einigen Anwendungen müssen Kunden möglicherweise zuerst andere abhängige Anwendungen wiederherstellen. Die Infrastruktur innerhalb des Vault kann die Recovery der größten Produktionsanwendung unterstützen, die von der Lösung geschützt wird.

Fazit

Unternehmen müssen bei der Erstellung eines Data-Protection-Konzepts viele Angriffsvektoren berücksichtigen. Dazu gehört der Schutz aller Daten, vor allem aber der für den Betrieb kritischen Daten. PowerProtect Cyber Recovery isoliert die kritischen Daten und trägt dazu bei, dass diese im Falle eines Cyberangriffs ordnungsgemäß wiederhergestellt werden können. Cyber Recovery nutzt ML-basierte Analysen in CyberSense, um die Integrität der Daten im Vault zu bestimmen und saubere Backupdaten für die Recovery zu identifizieren. In unseren Tests haben wir festgestellt, dass PowerProtect Cyber Recovery eine Infektion auf SQL-Datenbankseiten erkannt hat – was bei der Wettbewerberlösung nicht der Fall war. PowerProtect Cyber Recovery benötigte außerdem weniger Backups als die Wettbewerberlösung, um die Beschädigung der Daten zu ermitteln. Darüber hinaus bietet die Cyber Recovery-Lösung zahlreiche Recovery-Optionen, die sich auf unkompromittierte Daten aus dem Vault stützen, um eine effiziente und reibungslose Wiederaufnahme des Betriebs zu gewährleisten.

1. Dell, „CyberSense® für PowerProtect Cyber Recovery", abgerufen am 8. September 2023, https://www.delltechnologies.com/asset/en-in/products/data-protection/briefs-summaries/h18214-cybersense-for-dellemc-powerprotect-cyber-recovery-solution-brief.pdf.
2. Dell, „Dell PowerProtect Cyber Recovery Solution Guide", abgerufen am 23. August 2023, https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/h17670-cyber-recovery-sg.pdf.
3. Dell, „Dell PowerProtect Cyber Recovery Solution Guide".
4. Cohasset Associates, Inc, „Dell Technologies PowerProtect DD and DDVE – Compliance Assessment: SEC 17a-4(f), SEC 18a-6(e) and FINRA 4511(c)", abgerufen am 27. Oktober 2023, https://infohub.delltechnologies.com/section-assets/cohasset-dell-powerprotect-dd-compliance-assessment.
5. Dell, „Data Domain: Häufig gestellte Fragen zur Aufbewahrungssperre", abgerufen am 12. September 2023, https://www.dell.com/support/kbdoc/de-de/000079803/data-domain-retention-lock-h%C3%A4ufig-gestellte-fragen.
6. Dell, „Data Domain: Häufig gestellte Fragen zur Aufbewahrungssperre".
7. Dell, „Encryption Types Offered by DD Series Encryption Appliance", abgerufen am 8. September 2023, https://infohub.delltechnologies.com/l/powerprotect-dd-series-appliances-encryption-software-1/encryption-types-offered-by-dd-series-encryption-appliance.
8. Dell, „Dell EMC Data Domain – Sicherheitskonfigurationsleitfaden", abgerufen am 11. September 2023, https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/docu91808.pdf.
9. Dell, „Role based access control (RBAC) in Data Domain", Zugriff am 11. September 2023, https://www.dell.com/community/en/conversations/data-domain/role-based-access-control-rbac-in-data-domain/647f70a9f4ccf8a8dee30f99.
10. Dell, „Dell EMC Data Domain – Sicherheitskonfigurationsleitfaden".
11. Dell, „MTree Replication", abgerufen am 11. September 2023, https://infohub.delltechnologies.com/l/dell-powerprotect-cyber-recovery-reference-architecture/mtree-replication-3.

12. Veeam, „Dell EMC Data Domain – DataDomain MTree overview and limits“, abgerufen am 11. September 2023, https://bp.veeam.com/vbr/2_Design_Structures/D_Veeam_Components/D_backup_repositories/datadomain.html
13. Chris Wahl, „Recovering Fast from Ransomware Attacks: The Magic of an Immutable Backup Architecture“, abgerufen am 13. Dezember 2023, https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/rwp-recovering-fast-from-ransomware-attacks.pdf.
14. Veritas, „NetBackup™ Security and Encryption Guide“, abgerufen am 13. Dezember 2023, https://www.veritas.com/support/en_US/doc/21733320-149123528-0/v143394540-149123528.
15. Principled Technologies, „Dell EMC Cyber Recovery protected our test data from a cyber attack“, abgerufen am 21. August 2023, http://facts.pt/rkew01n.
16. Dell, „Dell PowerProtect Cyber Recovery“, abgerufen am 12. September 2023, https://www.delltechnologies.com/asset/de-de/products/data-protection/briefs-summaries/isolated-recovery-solution-overview.pdf.
17. Jerry Rozeman und Michael Hoeck, „Innovation Insight for Leveraging Isolated Recovery Environments and Immutable Data Vaults to Protect and Recover From Ransomware“, abgerufen am 14. Dezember 2023, https://www.gartner.com/doc/reprints?id=1-27MOHCBD&ct=211011&st=sb.
18. Jerry Rozeman und Michael Hoeck, „Innovation Insight for Leveraging Isolated Recovery Environments and Immutable Data Vaults to Protect and Recover From Ransomware“.
19. Nikitha Okmar, „Going Beyond the Air Gap – Data Isolation and Recovery for the Modern Era“, abgerufen am 13. Dezember 2023, https://www.cohesity.com/blogs/going-beyond-the-air-gap-data-isolation-and-recovery-for-the-modern-era/.
20. Marco Horstmann, „How to protect your data from ransomware and encryption Trojans“, abgerufen am 13. Dezember 2023, https://www.veeam.com/blog/how-to-protect-against-ransomware-data-loss-and-encryption-trojans.html.
21. Rubrik, „Rest easy with immutable, off-site data storage“, abgerufen am 13. Dezember 2023, https://www.rubrik.com/products/rubrik-cloud-vault.
22. Veritas, „NetBackup Isolated Recovery Environment“, abgerufen am 13. Dezember 2023, https://www.veritas.com/content/dam/www/en_us/documents/solution-overview/SO_flex_appliance_netbackup_ire_solution_V1543.pdf.
23. CSI Group, „Dell Cyber Recovery Vault (overview by CSI)“, abgerufen am 23. August 2023, https://youtu.be/ej5nZzWNRM0.
24. Dell, „Dell PowerProtect Cyber Recovery Solution Guide“.
25. Dell, „Dell PowerProtect Cyber Recovery Solution Guide“.
26. Dell, „CyberSense® für PowerProtect Cyber Recovery“.
27. Dell, „CyberSense® for Dell PowerProtect Cyber Recovery – Powered by Index Engines“, abgerufen am 13. September 2023, https://www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/cybersense-for-dell-powerprotect-cyber-recovery-whitepaper.pdf.
28. Index Engines, „CyberSense for Dell Cyber Recovery“, abgerufen am 25. September 2023, https://indexengines.com/csmatrix.
29. CISA, „#StopRansomware Guide“, abgerufen am 1. August 2023, https://www.cisa.gov/stopransomware/ransomware-guide.
30. „In security, most people use Shannon Entropy—a specific algorithm that returns a value between 0 and 8. The higher the number, the more random the data, and many times, a higher value means that the data is either packed or encrypted.“ Mueller, Clint, „How to Use Entropy Analysis in Penetration Testing“, 28. August 2023, https://www.schellman.com/blog/cybersecurity/penetration-testing-methods-entropy.
31. Cooper, Steven, „How to Protect Your Backups from Ransomware in 2023“, 1. August 2023, https://www.comparitech.com/net-admin/protect-backups-from-ransomware/.
32. Microsoft, „Pages and extents architecture guide“, abgerufen am 3. August 2023, https://learn.microsoft.com/en-us/sql/relational-databases/pages-and-extents-architecture-guide?view=sql-server-ver16.
33. W3 Schools, „SQL Injection“, abgerufen am 3. August 2023, https://www.w3schools.com/sql/sql_injection.asp.
34. Dell, „Dell PowerProtect Cyber Recovery Solution Guide“.
35. Dell, „Dell PowerProtect Cyber Recovery Solution Guide“.
36. Dell, „Dell PowerProtect Cyber Recovery Solution Guide“.

Lesen Sie den wissenschaftlichen Hintergrund dieses Berichts ▶

▶ Lesen Sie die Originalversion dieses Berichts in englischer Sprache unter https://facts.pt/64FU3b2.

Dieses Projekt wurde in Auftrag gegeben von Dell Technologies.

Principled Technologies®

Facts matter.®